UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/901,212	07/09/2001	Geoffrey S. Strongin	2000.054000	6397

23720 7590 09/08/2005

WILLIAMS, MORGAN & AMERSON, P.C.
10333 RICHMOND, SUITE 1100
HOUSTON, TX 77042

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

B

Office Action Summary	**Application No.** 09/901,212	**Applicant(s)** STRONGIN ET AL.	
	Examiner Aravind K. Moorthy	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 June 2005*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 July 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on 17 June 2005.

2. Claims 1-41 are pending in the application.

3. Claims 1-41 have been rejected.

Response to Amendment

4. The examiner approves of the amendment made to claims 12 and 13. The applicant has deleted the word "modem" from the claim. This amendment overcomes the claim rejections 35 USC § 112 (2) of lack of antecedent basis. The examiner withdraws the rejection.

Response to Arguments

5. Applicant's arguments filed 17 June 2005 have been fully considered but they are not persuasive.

On page 15, the applicant argues that Beckert et al does not describe or suggest a processing unit adapted to execute a driver, in the sense that the term "driver" is used in the present application.

The examiner respectfully disagrees. Beckert et al teaches a "multimedia driver" which is used in sense that the term "driver" is used in the present application.

On page 15, the applicant argues that Beckert et al fails to describe or suggest a driver for interfacing with the peripheral device in a standard mode of operation and an authentication agent in a privileged mode of operation, as set forth in independent claim 1.

The examiner respectfully disagrees. As discussed above Becker et al teaches a "multimedia driver". The "multimedia driver" is interfaced with peripheral devices in a standard mode of operation and an authentication agent in a privileged mode of operation, as set forth in independent claim 1.

On page 15, the applicant argues that Beckert et al fails to provide any suggestion or motivation to modify the prior art to arrive at the applicant's claimed invention.

The examiner respectfully disagrees. Beckert et al does not teach any method of authenticating a driver. Moore provides the motivation proving that the driver is indeed authentic and has not been modified.

On page 16, the applicant argues that Jain is completely silent with regard to standard and privileged modes of operation.

The examiner respectfully disagrees. Jain teaches a non-secure mode of operation and an authenticated mode of operation.

On pages 16 and 17, the applicant argues that Jain does not describe or suggest a processing unit adapted to execute a modem driver in a standard mode and an authentication agent in a privileged mode of operation.

The examiner respectfully disagrees. As discussed above, Jain teaches a standard mode and an authentication agent in a privileged mode of operation. Jain teaches the driver of the communication unit which is a modem.

On page 17, the applicant argues that Jain provides no suggestion or motivation to modify the prior art to arrive at the applicant's claimed invention.

The examiner respectfully disagrees. The examiner respectfully disagrees. Jain does not teach any method of authenticating a driver. Moore provides the motivation proving that the driver is indeed authentic and has not been modified.

On page 18, the applicant argues that Scherf is completely silent with regard to any particular operating modes of the system.

The examiner respectfully disagrees. Scherf teaches different operating modes of the driver.

On page 18, the applicant argues that Scherf fails to teach or suggest executing a driver in standard processing mode of a processing unit and transitioning the processing unit into a privileged mode, as set forth in claim 34.

The examiner respectfully disagrees. Scherf teaches different operating modes. Scherf teaches the driver operating in a secure mode.

On page 18, the applicant argues that Scherf fails to describe or suggest authenticating the driver in the privileged mode, as set forth in claim 34.

The examiner respectfully disagrees. Scherf teaches authenticating the driver in secure mode with a hashing function.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1, 2, 5-11, 14 and 15 are rejected under 35 U.S.C. 102(b) as being anticipated by Beckert et al U.S. Patent No. 5,794,164.

As to claim 1, Beckert et al discloses a computer system, comprising:

a peripheral device [column 3 line 66 to column 4 line 9];

a processing unit adapted to execute a driver for interfacing with the peripheral device in a standard mode of operation and an authentication agent in a privileged mode of operation, wherein the authentication agent includes program instructions adapted to authenticate the driver [column 9, lines 36-54].

As to claim 2, Beckert et al discloses that the authentication agent includes program instructions adapted to signal a security violation in response to a driver authentication failure [column 9, lines 36-54].

As to claim 5, Beckert et al discloses that the processing unit includes a timer adapted to generate an interrupt signal for invoking the authentication agent after a predetermined interval [column 10, lines 8-23].

As to claim 6, Beckert et al discloses that the driver includes program instructions adapted to periodically invoke the authentication agent [column 10, lines 8-23].

As to claim 7, Beckert et al discloses that the privileged mode of operation comprises a system management mode of operation [column 9, lines 36-54].

As to claim 8, Beckert et al discloses that the driver includes program instructions adapted to issue a signal to the processing unit to initiate a change from the standard mode of operation to the privileged mode of operation [column 9, lines 36-54].

As to claim 9, Beckert et al discloses that the signal comprises a system management interrupt [column 10, lines 24-37].

As to claim 10, Beckert et al discloses a system basic input output system (BIOS) memory adapted to store the authentication agent [column 8 line 62 to column 9 line 16].

As to claim 11, Beckert et al discloses that the processing unit is adapted to load the authentication agent from the system BIOS into a protected memory location during initialization of the computer system [column 8 line 62 to column 9 line 16].

As to claim 14, Beckert et al discloses that the authentication agent includes program instructions adapted to prohibit further operation of the driver in response to identifying the security violation [column 9, lines 36-54].

As to claim 15, Beckert et al discloses that the authentication agent includes program instructions adapted to prohibit further operation of the processing unit in response to identifying the security violation [column 9, lines 36-54].

7. Claims 16, 17, 20, 21, 23-29, 32 and 33 are rejected under 35 U.S.C. 102(e) as being anticipated by Jain U.S. Patent No. 6,367,018 B1.

As to claim 16, Jain discloses a communications system, comprising:

> a physical layer hardware unit adapted to communicate data over a communications channel in accordance with assigned transmission parameters, the physical layer hardware unit being adapted to receive an incoming signal over the communications channel and sample the incoming signal to generate a digital received signal [column 4, lines 12-29]; and

> a processing unit adapted to execute a modem driver in a standard mode of operation and an authentication agent in a privileged mode of operation, wherein the standard mode driver includes program instructions adapted to extract control codes from the digital received signal and configure the physical layer hardware assigned transmission parameters based on the control codes, and the authentication agent includes program instructions adapted to authenticate the modem driver [column 4, lines 30-43].

As to claim 17, Jain discloses that the authentication agent includes program instructions adapted to signal a security violation in response to a modem driver authentication failure [column 5 line 43 to column 6 line 5].

As to claim 20, Jain discloses that the processing unit includes a timer adapted to generate an interrupt signal for invoking the authentication agent after a predetermined interval [column 6, lines 31-49].

As to claim 21, Jain discloses that the modem driver includes program instructions adapted to periodically invoke the authentication agent [column 6, lines 11-29].

As to claim 23, Jain discloses that the privileged mode of operation comprises a system management mode of operation [column 5 line 43 to column 6 line 5].

As to claim 24, Jain discloses that the modem driver includes program instructions adapted to issue a signal to the processing unit to initiate a change from the standard mode of operation to the privileged mode of operation [column 5 line 43 to column 6 line 5].

As to claim 25, Jain discloses that the signal comprises a system management interrupt [column 6, lines 31-49].

As to claim 26, Jain discloses that the processing unit comprises a computer [column 4, lines 12-28].

As to claim 27, Jain discloses that the computer includes:

a processor complex adapted to execute the program instructions in the modem driver and the authentication agent [column 4, lines 30-43];

a bus coupled to the processor complex [column 4, lines 30-43]; and

an expansion card coupled to the bus, the expansion card including the physical layer hardware [column 4, lines 30-43]

As to claim 28, Jain discloses that the computer includes a system basic input output system (BIOS) memory adapted to store the authentication agent [column 5, lines 9-34].

As to claim 29, Jain discloses that the computer is adapted to load the privileged mode driver from the system BIOS into a protected memory location during initialization of the computer [column 5, lines 9-34].

As to claim 32, Jain discloses that the authentication agent includes program instructions adapted to prohibit further operation of the modem driver in response to identifying the security violation [column 5 line 43 to column 6 line 5].

As to claim 33, Jain discloses that the authentication agent includes program instructions adapted to prohibit further operation of the processing unit in response to identifying the security violation [column 5 line 43 to column 6 line 5].

8. Claims 34-41 are rejected under 35 U.S.C. 102(b) as being anticipated by Scherf U.S. Patent No. 5,390,301.

As to claims 34 and 41, Scherf discloses a method for identifying security violations in a computer system, comprising:

executing a driver in a standard processing mode of a processing unit [column 5, lines 9-27];

transitioning the processing unit into a privileged processing mode [column 5, lines 28-38]; and

authenticating the driver in the privileged processing mode [column 5, lines 28-38].

As to claim 35, Scherf discloses signaling a security violation in response to a driver authentication failure [column 6, lines 1-21].

As to claim 36, Scherf discloses that authenticating the driver includes:

generating a hash of at least a portion of the driver [column 5, lines 9-27];

decrypting a digest associated with the driver [column 5, lines 54-67]; and

comparing the hash to the digest to authenticate the driver [column 5, lines 54-67].

As to claim 37, Scherf discloses that decrypting the digest comprises decrypting the digest using a public key [column 5, lines 54-67].

As to claim 38, Scherf discloses generating an interrupt signal for authenticating the driver in the privileged processing mode after a predetermined interval [column 6, lines 1-21].

As to claim 39, Scherf discloses prohibiting further operation of the driver in response to identifying the security violation [column 5, lines 54-67].

As to claim 40, Scherf discloses prohibiting further operation of the processing unit in response to identifying the security violation [column 5, lines 54-67].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 3, 4, 12 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beckert et al U.S. Patent No. 5,794,164 as applied to claim 1 above, and further in view of Moore U.S. Patent No. 5,343,527.

As to claims 3 and 4, Beckert et al does not teach that the authentication agent includes program instructions adapted to generate a hash of at least a portion of the driver, decrypt a digest associated with the driver, and compare the hash to the digest to authenticate the driver. Beckert et al does not teach that the authentication agent includes program instructions adapted to decrypt the digest associated with the driver using a public key.

Moore teaches generating a hash of at least a portion of a software component, decrypt a digest associated with the software component, and compare the hash to the digest to authenticate the software component [column 7, lines 31-38]. Moore teaches that the decrypting the digest associated with the software component using a public key [column 13, lines 13-37].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Beckert et al so that the driver was authenticated by means of generating a hash on the driver. A digest associated with the driver would have been decrypted. The hash would have been compared with the digest to authenticate the driver. The digest would have been decrypted with a public key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Beckert et al by the teaching of Moore because it provides a system that proves that the driver is indeed authentic and has not been modified. It also prevents a third party from passing off the driver as that of another [column 2, lines 13-27].

As to claim 12, Beckert et al does not teach that the authentication agent includes program instructions adapted to generate a hash of at least a portion of the driver, decrypt a digest associated with the driver using a public key, and compare the hash to the digest to authenticate the driver. Beckert et al does not teach that the system further comprises a system basic input output system (BIOS) memory adapted to store the public key.

Moore teaches generating a hash of at least a portion of a software component, decrypt a digest associated with the software component, and compare the hash to the digest to authenticate the software component [column 7, lines 31-38]. Moore teaches that the decrypting the digest associated with the software component using a public key [column 13, lines 13-37].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Beckert et al so that the driver was authenticated by means of generating a hash on the driver. A digest associated with the driver would have been decrypted. The hash would have been compared with the digest to authenticate the driver.

The digest would have been decrypted with a public key. The basic input output system (BIOS) would have stored the public key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Beckert et al by the teaching of Moore because it provides a system that proves that the driver is indeed authentic and has not been modified. It also prevents a third party from passing off the driver as that of another [column 2, lines 13-27].

As to claim 13, Beckert et al does not teach that the authentication agent includes program instructions adapted to generate a hash of at least a portion of the driver, decrypt a digest associated with the driver using a public key, and compare the hash to the digest to authenticate the driver. Beckert et al does not teach that the peripheral device includes a memory device adapted to store the public key.

Moore teaches generating a hash of at least a portion of a software component, decrypt a digest associated with the software component, and compare the hash to the digest to authenticate the software component [column 7, lines 31-38]. Moore teaches that the decrypting the digest associated with the software component using a public key [column 13, lines 13-37].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Beckert et al so that the driver was authenticated by means of generating a hash on the driver. A digest associated with the driver would have been decrypted. The hash would have been compared with the digest to authenticate the driver. The digest would have been decrypted with a public key. The peripheral device would have stored the public key in its memory device.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Beckert et al by the teaching of Moore because it provides a system that proves that the driver is indeed authentic and has not been modified. It also prevents a third party from passing off the driver as that of another [column 2, lines 13-27].

10. Claims 18, 19 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jain U.S. Patent No. 6,367,018 B1 as applied to claim 16 above, and further in view of Moore U.S. Patent No. 5,343,527.

As to claims 18 and 19, Jain does not teach that the authentication agent includes program instructions adapted to generate a hash of at least a portion of the modem driver, decrypt a digest associated with the modem driver, and compare the hash to the digest to authenticate the modem driver. Jain does not teach that the authentication agent includes program instructions adapted to decrypt the digest associated with the modem driver using a public key.

Moore teaches generating a hash of at least a portion of a software component, decrypt a digest associated with the software component, and compare the hash to the digest to authenticate the software component [column 7, lines 31-38]. Moore teaches that the decrypting the digest associated with the software component using a public key [column 13, lines 13-37].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jain so that the modem driver was authenticated by means of generating a hash on the driver. A digest associated with the modem driver would have been decrypted. The hash would have been compared with the digest to authenticate the modem driver. The digest would have been decrypted with a public key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jain by the teaching of Moore because it provides a system that proves that the driver is indeed authentic and has not been modified. It also prevents a third party from passing off the driver as that of another [column 2, lines 13-27].

As to claim 31, Jain does not teach that the authentication agent includes program instructions adapted to generate a hash of at least a portion of the modem driver, decrypt a digest associated with the modem driver, and compare the hash to the digest to authenticate the modem driver. Jain does not teach that the authentication agent includes program instructions adapted to decrypt the digest associated with the modem driver using a public key. Jain does not teach that the expansion card includes a memory device adapted to store the public key.

Moore teaches generating a hash of at least a portion of a software component, decrypt a digest associated with the software component, and compare the hash to the digest to authenticate the software component [column 7, lines 31-38]. Moore teaches that the decrypting the digest associated with the software component using a public key [column 13, lines 13-37].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jain so that the modem driver was authenticated by means of generating a hash on the driver. A digest associated with the modem driver would have been decrypted. The hash would have been compared with the digest to authenticate the modem driver. The digest would have been decrypted with a public key. The public key would have been stored in the expansion card that would have included a memory device.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jain by the teaching of Moore because it provides a system that proves that the driver is indeed authentic and has not been modified. It also prevents a third party from passing off the driver as that of another [column 2, lines 13-27].

11. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jain U.S. Patent No. 6,367,018 B1 as applied to claim 16 above, and further in view of Fleming, III et al U.S. Patent No. 6,212,360 B1.

As to claim 22, Jain does not teach that the control codes include at least one of a power level assignment, a frequency assignment, and a time slot assignment.

Fleming, III et al teaches control codes that include at least one of a power level assignment, a frequency assignment, and a tune slot assignment [column 11 line 60 to column 12 line 13].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jain so that the control code would have been power level assignment.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jain by the teaching of Fleming, III et al because adjusting power in the modem it helps overcome rain fades in wireless or satellite systems [column 2, lines 39-46].

12. Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jain U.S. Patent No. 6,367,018 B1 as applied to claim 16 above, and further in view of Moore U.S. Patent No. 5,343,527 and Labatte et al U.S. Patent No. 5,901,311.

As to claim 30, Jain does not teach that the authentication agent includes program instructions adapted to generate a hash of at least a portion of the modem driver, decrypt a digest associated with the modem driver, and compare the hash to the digest to authenticate the modem driver. Jain does not teach that the authentication agent includes program instructions adapted to decrypt the digest associated with the modem driver using a public key. Jain does not teach that the expansion card includes a memory device adapted to store the public key. Jain does not teach a system basic input output system (BIOS) memory adapted to store the public key.

Moore teaches generating a hash of at least a portion of a software component, decrypt a digest associated with the software component, and compare the hash to the digest to authenticate the software component [column 7, lines 31-38]. Moore teaches that the decrypting the digest associated with the software component using a public key [column 13, lines 13-37].

Labatte et al teaches storing a key in the BIOS [column 10, lines 6-13].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jain so that the modem driver was authenticated by means of generating a hash on the driver. A digest associated with the modem driver would have been decrypted. The hash would have been compared with the digest to authenticate the modem driver. The digest would have been decrypted with a public key. The public key would have been stored in the system basic input output system (BIOS) memory.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jain by the teaching of Moore because it provides a system that proves that the driver is indeed authentic and has not been modified. It also prevents a third party from passing off the driver as that of another [column 2, lines 13-27]. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jain by the teaching of Labatte et al because it prevents unauthorized users from finding the key in the BIOS.

Conclusion

13. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
September 1, 2005

Primary Examiner
AU 2131
9/2/05